UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/607,562	06/25/2003	Karl L. Ginter	7451.0001-22	7288

22852 7590 06/17/2005

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
DARROW, JUSTIN T	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

5

Office Action Summary	**Application No.** 10/607,562	**Applicant(s)** GINTER ET AL.	
	Examiner Justin T. Darrow	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _25 June 2003_.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _91-129_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _91-129_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _25 June 2003_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-129 have been presented for examination. Claims 1-90 have been canceled and claims 91-129 have been copied from U.S. Patent No. 6,412,070 B1 in order to provoke an interference. Claims 91-129 have been examined.

Priority

2. Acknowledgment is made that the instant application is a continuation of Application No. 09/698,044, filed 10/30/2000, which is a continuation of Application No. 09/208,017, filed 12/09/1998, now U.S. Patent No. 6,253,193 B1, which is a continuation of Application No. 08/964,333, filed 11/04/1997, now U.S. Patent No. 5,982,891 A, which is a continuation of Application No. 08/388,107, filed 02/13/1995, now abandoned.

3. It is noted that this application appears to claim subject matter disclosed in prior Application No. 08/964,333, filed 11/04/1997. Although a reference to this prior application has been inserted as the first sentence of the specification of this application by an amendment filed 06/25/2003, the reference is missing the filing date of the application of 11/04/1997.

Information Disclosure Statement

4. The information disclosure statement (IDS) submitted on 05/27/2003 was filed before the mailing date of the first Office action on the merits. The submission is in compliance with the provisions of 37 CFR 1.97(b)(3). Accordingly, the information disclosure statement is being considered by the examiner.

Claim Objections

5. Claim 102 is objected to because of the following informalities: after "object;" in line 6, insert --and--.

6. Claim 119 is objected to because of the following informalities: after "list;" in line 6, insert --and--.

Interference

7. Claims 91-129 of this application has been copied from U.S. Patent No. 6,412,070 B1 for the purpose of an interference.

Applicant has failed to specifically apply each limitation or element of each of the copied claim to the disclosure of the application.

Applicant is given ONE MONTH or THIRTY DAYS, whichever is longer, from the mailing date of this communication to specifically apply each limitation or element of each of the copied claim(s) to the disclosure of the application. See 37 CFR 41.202(a)(5), 69 *Fed. Reg.* 50019 (08/12/2004). THE PROVISIONS OF 37 CFR 1.136 DO NOT APPLY TO THE TIME SPECIFIED IN THIS ACTION.

8. Applicant has failed to provide a claim chart showing how the claims correspond to those copied from U.S. Patent No. 6,412,070 B1. See 37 CFR 41.202(a)(3), 69 *Fed. Reg.* 50019 (08/12/2004).

9. Applicant has failed to explain in detail why the applicant will prevail on priority. See 37 CFR 41.202(a)(4), 69 *Fed. Reg.* 50019 (08/12/2004).

Claim Rejections - 35 USC § 112

10. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claims 119-129 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 119-129 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See MPEP § 2172.01. The omitted elements are: structural features for a computing system for authorizing a security principal to access one or more operations of an individual object.

Claims 119-129 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. The omitted structural cooperative relationships are: structural cooperative relationships for a computing system for authorizing a security principal to access one or more operations of an individual object.

Claim Rejections - 35 USC § 101

12. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

13. Claims 91-101 and 113-129 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

14. Claims 91-96 are drawn to a computer-readable medium having stored thereon a control access data structure. Although independent claim 91 recites that the control access data structure corresponds to an access control entry of one or more objects within a computing environment, where the access control entry associates an access right to an operation on the one or more objects, with a trusted user, claim 91 does not specify that the access control entry is used by the computing environment to grant the trusted user the access right to the one or more objects. The recited control access data structure, access control entry, the identification field for storing a unique identifier of the control access data structure, and the one or more object identification fields represent descriptive material with no functional interrelationship with the way in which computing processes are performed. See MPEP § 2106 IV B. 1 (b). Nonfunctional descriptive material is nonstatutory. *Id.* The recited data structures and associated information must be claimed to define functional characteristics through the structural elements of the computing environment. See *In re Lowry*, 32 USPQ2d 1031, 1033-34 (Fed. Cir. 1994) (claiming a memory for storing a data structure used by an application program executed on a data processing system establishing a hierarchy of attribute data objects). As a matter of policy, the claimed computer-readable medium as an article of manufacture with the nonfunctional descriptive material of claims 91-96 is still unpatentable under 35 U.S.C. 101 because the purely nonfunctional descriptive material cannot alone provide the practical application for the manufacture. See MPEP § 2106 IV B. 1 (b).

15. Claims 97-101 are drawn to a computer program. Data structures not claimed as embodied in computer-readable media are descriptive material *per se* and are not statutory because they are not capable of causing functional change in the computer. See MPEP § 2106 IV B. 1 (a) and In re *Warmerdam*, 31 USPQ2d 1754, 1760 (claim to a data structure *per se* held nonstatutory). Such claimed data structures do not define any structural and functional interrelationships between the data structure and other claimed aspects of the invention which permit the data structure's functionality for granting a user permission corresponding to a desired operation on an object to be realized. See MPEP § 2106 IV B. 1 (a). In contrast, a claimed computer-readable medium encoded with a data structure defines structural and functional interrelationships between the data structure and the computer software and hardware components which permit the data structure's functionality to be realized, and is thus statutory. *Id.*

16. Claims 113 and 114-118 are drawn to one or more computer-readable media comprising computer executable instructions to perform a method and one or more computer-readable media maintaining an extensible control access right, respectively. Claims drawn to many parts, such as computer-readable media, is not a "manufacture" unless it is a group or "kit" of interrelated parts. See *In re Venezia*, 189 USPQ 149, 153 (C.C.P.A. 1976). Therefore, claims drawn to one or more computer readable media is nonstatutory.

17. Claims 114-118 are drawn to one or more computer-readable media maintaining an extensible control access right. Although independent claim 114 recites that the control access data structure defines access by an authorized security principal to one or more operations of an object within a computing environment, claim 114 does not specify the computing environment uses the control access data structure to grant access to the authorized security principal to the one or more operations of the object. The recited control access data structure, access control entry, the identification field for storing a unique identifier of the control access data structure, and the object identification field to maintain a unique object identifier represent descriptive material with no functional interrelationship with the way in which computing processes are performed. See MPEP § 2106 IV B. 1 (b). Nonfunctional descriptive material is nonstatutory. *Id.* The recited data structures and associated information must be claimed to define functional characteristics through the structural elements of the computing environment. See *In re Lowry*, 32 USPQ2d 1031, 1033-34 (Fed. Cir. 1994) (claiming a memory for storing a data structure used by an application program executed on a data processing system establishing a hierarchy of attribute data objects). As a matter of policy, the claimed computer-readable medium as an article of manufacture with the nonfunctional descriptive material of claims 114-118 is still unpatentable under 35 U.S.C. 101 because the purely nonfunctional descriptive material cannot alone provide the practical application for the manufacture. See MPEP § 2106 IV B. 1 (b).

18. Claims 119-129 are drawn to a computer system comprising data structures not claimed as structural elements in a machine. Data structures not claimed as embodied in computer-readable media are descriptive material *per se* and are not statutory because they are not capable

of causing functional change in the computer. See MPEP § 2106 IV B. 1 (a) and In re *Warmerdam*, 31 USPQ2d 1754, 1760 (claim to a data structure *per se* held nonstatutory). Such claimed data structures do not define any structural and functional interrelationships between the data structure and other claimed aspects of the invention which permit the data structure's functionality for authorizing a security principal to access one or more operations of an individual object to be realized. See MPEP § 2106 IV B. 1 (a). In contrast, a claimed combination of interrelated elements which combine to form a machine for authorizing a security principal to access one or more operations of an individual object is statutory. See MPEP § 2106 IV B. 2 (a) and *In re Alappat*, 31 USPQ2d 1545, 1557 (Fed. Cir. 1994) (en banc).

19. To expedite a complete examination of the application, the claims rejected under 35 U.S.C. 101 (nonstatutory) above are further rejected as set forth below in anticipation of count(s) placed within the four statutory categories of invention.

Claim Rejections - 35 USC § 102

20. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

21. Claims 91-129 are rejected under 35 U.S.C. 102(e) as being anticipated by Fischer, U.S. Patent No. 5,412,717 A.

As per claim 91, Fischer illustrates a computer-readable medium having stored thereon a control access data structure for defining an access right to an operation of one or more objects within a computing environment (see column 4, lines 55-58; figure 1, item 7; non-volatile program and program authorization information (PAI) storage; see column 5, lines 3-7; figure 2; storing a program authorization information (PAI) data structure; column 5, lines 55-67; figure 2, segments 34 and 36; with segments to identify functions on specific files and/or class of files), the control access data structure comprising:

an identification field for storing a unique identifier of the control access data structure (see column 7, lines 28-35; figure 3A, item 84; a program related identifier indicating the associated program authorization information PAI 1; see column 7, lines 35-42; such as a digital signature of the program authorization information);

one or more object identification fields for associating the control access data structure with the one or more objects of the computing environment (see column 5, lines 63-66; figure 2, segment 36; specific user files designated in a segment); and

wherein the control access data structure corresponds to an access control entry of the one or more objects (see column 5, lines 55-67; figure 2, segments 34 and 36; segments that specify the kind of access and use of a file like a program and the particular files; see column 6, lines 8-10; such as alter a program file), and wherein the access control entry associates the access right with a trusted user of the computing environment (see column 8, lines 45-49; figure 3D, item 129; user-distinct Program Authorization Information; see column 8, lines 55-57; allowing different users different limited access to program files).

As per claim 92, Fischer further points out:

that an individual object identification field of the control access data structure stores a unique identifier of an associated object (see column 5, lines 63-66; figure 2, segment 36; specific user files are designated in a segment).

As per claim 93, Fischer additionally describes:

one or more access control entries (ACE's), wherein each ACE includes a rights field for associating the control access data structure with one or more objects (see column 8, lines 3-11; figure 3C, segment 118; object program segments to control the manner in which an associated file is presented and manipulated to a particular user).

As per claim 94, Fischer then specifies:

that the rights field of each ACE stores the unique identifier of the control access data structure (see column 8, lines 25-44; figure 3C, segment 120; a data segment containing the digital signature of the program authorization information).

As per claim 95, Fischer next explains:

that each ACE further includes a trusted user field for associating an ACE with the trusted user of the computing environment (see column 8, lines 3-7 and 16-20; figure 3C, segment 118; a field designating a recipient of the program as a user that may use the file in a particular manner).

As per claim 96, Fischer moreover suggests:

the trusted user field of each ACE stores a unique identifier of the trusted user (see column 8, lines 16-17; figure 3C, segment 118; segment designates a recipient as a trusted user).

As per claim 97, Fischer depicts a computer program comprising:

means for defining an access right component that defines a permission corresponding to a desired operation of the object (see column 11, lines 40-61; figure 6, steps 212, 214, and 216; determine file access authority with respect to any fields or elements in a file to a particular type of access to the file);

means for associating the access right component with the object (see column 11, lines 48-50; figure 6, step 214; file access authority associated with the file(s) by file name, file stem, or "wild card" file name pattern);

means for associating the access right component with an access control entry corresponding to the object (see column 11, lines 67-68; column 12, lines 1-9; figure 6, steps 218 and 221; determining programs that can be invoked under limitations and qualifications; see column 11, lines 55-64; figure 6, step 216; to achieve a type of file access); and means for associating the access right component with a user in order to grant the desired operation (see column 13, lines 61-64; figure 7, step 233; the authority to execute programs to access files based on qualifications of the user).

As per claim 98, Fischer further describes:

an administrative tool for controlling the defining means (see column 11, lines 7-9; figures 6-9; a utility program for establishing program authorization information).

As per claim 99, Fischer additionally discloses:

an interface for allowing a user application to programmatically control the defining means (see column 11, lines 9-13; the utility program prompts the end user to define a range of authorities associated with a program).

As per claim 100, Fischer then points out:

that the means for associating the access right component with the object includes means for storing a unique identifier of the object within a field of a control access data structure created by the defining means (see column 11, lines 40-50; figure 6, steps 212 and 214; a determination of the file access authority results in the user being prompted to specify a file name or a file stem, or "wild card" file name pattern).

As per claim 101, Fischer also shows:

that the means for associating the access right component with the user (see column 13, lines 61-64; figure 7, step 233; the authority to execute programs to access files based on qualifications of the user) includes:

means for adding the access control entry (ACE) to an access control list (ACL) that corresponds to the object (see column 13, lines 64-68; column 14, line 1; figure 7, steps 232 and 234; determination that certain programs for operation on files be given special memory access to those files; see column 8, lines 3-11; figure 3C, segment 118; object program segments to control the manner in which an associated file is presented and manipulated to a particular user);

means for storing a unique identifier of a control access data structure within a first field of the ACE (see column 12, lines 66-68; column 13, lines 1-10; creating and storing the digital signature of the program authorization information PAI; see column 8, lines 25-44; figure 3C, segment 120; a data segment containing the digital signature of the program authorization information); and

means for storing a unique identifier of the user within a second field of the ACE (see column 14, lines 4-17; figure 7, step 238; adding a requirement for user to enter a secret password for operation; see column 8, lines 16-17; figure 3C, segment 116; segment designates a recipient as a trusted user).

As per claims 102 and 113, Fischer illustrates a method and one or more computer-readable media comprising executable instructions that, when executed, direct a computing system (see column 4, lines 55-58; figure 1, items 2 and 7; a processor coupled to non-volatile program and program authorization information (PAI) storage; see column 11, lines 7-13; figures

6-9; to implement a utility program for establishing program authorization information) to perform the method comprising:

creating an access control entry as a component of an access control list that is associated with at least one object in a computing environment (see column 11, lines 67-68; column 12, lines 1-9; figure 6, steps 218 and 221; determining programs that can be invoked under limitations and qualifications; see column 11, lines 55-64; figure 6, step 216; to achieve a type of file access; see column 8, lines 3-11; figure 3C, segment 118; where the object program segments to control the manner in which an associated file is presented to and manipulated by a particular user are stored in a data structure),

where the access control entry identifies a security principal (see column 11, lines 65-67; figure 6, step 218; determining a program to invoke other programs);

defining an extensible access right component that defines access to one or more operations of the at least one object (see column 11, lines 40-61; figure 6, steps 212, 214, and 216; determine file access authority with respect to any fields or elements in a file to a particular type of access to the file for operations such as reading from files, inserting information into files, updating information in files, deleting information from files, erasing files, transmitting a file, etc.); and

associating the extensible access right component with the access control entry such that the security principal is authorized to access the one or more operations of the at least one object (see column 12, lines 2-9; see figure 6, steps 218 and 221; determining limitations or qualifications by which the program can invoke other programs to operate on files by either file names of the programs or a specification of a library, where the programs reside).

As per claim 103, Fischer further mentions:

defining includes creating the extensible access right component as a component of the access control entry (see column 12, lines 2-9; see figure 6, steps 218 and 221; determining limitations or qualifications by which the program can invoke other programs to operate on files by either file names of the programs or a specification of a library, where the programs reside; see column 12, lines 24-44; in terms of a specification distinguishing elements by any appropriate attribute, method, or criteria in terms of segments in the program authorization information PAI as contiguous or discontiguous segments of data).

As per claim 104, Fischer then specifies:

defining the extensible access right component includes defining access to a property of the at least one object (see column 12, lines 2-9; see figure 6, steps 218 and 221; determining limitations or qualifications concerning operations on files; see column 12, lines 24-44; in terms of a specification distinguishing elements by any appropriate attribute).

As per claim 105, Fischer also points out:

defining the extensible access right component includes defining access to a method exposed by at least one object (see column 12, lines 2-9; see figure 6, steps 218 and 221; determining limitations or qualifications concerning operations on files; see column 12, lines 24-44; in terms of a specification distinguishing elements by any appropriate method).

As per claim 106, Fischer then specifies:

defining the extensible access right component includes defining access to a property of the at least one object (see column 12, lines 2-9; see figure 6, steps 218 and 221; determining limitations or qualifications concerning operations on files; see column 12, lines 24-44; in terms of a specification distinguishing elements by any appropriate attribute), and

associating includes association the extensible access right component with the security principal such that the security principal is authorized to access the property of the at least one object (see column 11, lines 55-67; figure 6, steps 216, 218, and 221; the program as a security principal can invoke other programs to access a property of a file such as updating information in a file in accessing the version to revise the file, or insert information into the file to access the size of the file, etc.).

As per claim 107, Fischer also points out:

defining the extensible access right component includes defining access to a method exposed by at least one object (see column 12, lines 2-9; see figure 6, steps 218 and 221; determining limitations or qualifications concerning operations on files; see column 12, lines 24-44; in terms of a specification distinguishing elements by any appropriate method), and

associating includes association the extensible access right component with the security principal such that the security principal is authorized to initiate the method (see column 11, lines 55-67; figure 6, steps 216, 218, and 221; the program as a security principal can invoke other programs to begin reading from files, inserting information into files, deleting information from files, erasing files, transmitting a file, etc.).

As per claim 108, Fischer moreover discusses:

defining including an application executing in the computing environment defining the extensible access right component (see column 11, lines 7-9; a utility program for establishing program authorization information; see column 11, lines 40-61; figure 6, steps 212, 214, and 216; determining file access authority with respect to a particular type of access to a file).

As per claim 109, Fischer moreover discusses:

defining including an application executing in the computing environment defining the extensible access right component as a component of the access control entry (see column 11, lines 7-9; a utility program for establishing program authorization information; see column 11, lines 40-61; figure 6, steps 212, 214, and 216; determining file access authority with respect to a particular type of access to a file; see column 11, lines 67-68; column 12, lines 1-9; figure 6, steps 218 and 221; through programs that can be invoked under limitations and qualifications; see column 11, lines 55-64; figure 6, step 216; to achieve a type of file access).

As per claim 110, Fischer additionally mentions:

defining including creating a control access data structure (see column 11, lines 7-13; figures 6-9; defining a range of authorities by establishing program authorization information (PAI)0, and

associating including maintaining a unique identifier of the at least one object with the control access data structure (see column 11, lines 40-50; figure 6, steps 212 and 214; a determination of the file access authority with specifying a file name or a file stem, or "wild card" file name pattern).

As per claim 111, Fischer then discusses:

associating including the access control entry maintaining a unique identifier of the extensible access right component (see column 11, lines 67-68; column 12, lines 1-9; figure 6, steps 218 and 221; determining programs that can be invoked under limitations and qualifications; see column 11, lines 55-64; figure 6, step 216; to achieve a type of file access expressly specified by the user).

As per claim 112, Fischer also describes:

associating including the access control entry maintaining a unique identifier of the control access data structure that represents the extensible access right component (see column 12, lines 66-68; column 13, lines 1-10; creating and storing the digital signature of the program authorization information PAI; see column 8, lines 25-44; figure 3C, segments 116 and 118; a data segment containing the digital signature of the program authorization information stored with program segments that accommodate different uses of the object file).

As per claim 114, Fischer shows one or more computer-readable media maintaining an extensible control access right (see column 4, lines 55-58; figure 1, item 7; non-volatile program and program authorization information (PAI) storage; see column 5, lines 3-7; figure 2; storing a program authorization information (PAI) data structure; column 5, lines 55-67; figure 2, segments 34 and 36; with segments to identify functions on specific files and/or class of files), comprising:

a control access data structure (see column 5, lines 3-7; figure 2; storing a program authorization information (PAI) data structure; column 5, lines 55-67; figure 2, segments 34 and 36; with segments to identify functions on specific files and/or class of files) that includes:

an identification field for storing a unique identifier of the control access data structure (see column 7, lines 28-35; figure 3A, item 84; a program related identifier indicating the associated program authorization information PAI 1; see column 7, lines 35-42; such as a digital signature of the program authorization information);

an object identification field to maintain a unique identifier of an object within a computing environment, configured to associate the control access data structure with the object (see column 5, lines 63-66; figure 2, segment 36; specific user files designated in a segment); and

wherein the control access data structure defined access by an authorized security principal to one or more operations of the object (see column 6, lines 12-18; figure 2, segment 38; a segment specifying the level of authority which has been granted to a program as a security principal to permit certain operations on a predetermined set of files, such as reading, but denying the authority to alter, or delete any such files).

As per claim 115, Fischer further describes:

that the control access data structure further includes at least one other object identification field to maintain a second unique identifier of at least one other object within the computing environment, configured to associate the control access data structure with the one other object (see column 5, lines 63-66; figure 2, segment 36; specific user files designated in a segment).

As per claim 116, Fischer additionally points out:

the extensible control access right further comprising an access control entry that is associated with the object (see column 8, lines 3-11; figure 3C, segment 118; object program segments to control the manner in which an associated file is presented and manipulated to a particular user),

configured to maintain the unique identifier of the control access data structure to associate the control access data structure with the object (see column 8, lines 25-44; figure 3C, segment 120; a data segment containing the digital signature of the program authorization information).

As per claim 117, Fischer then shows:

the extensible control access right further comprising an access control entry that is associated with the object (see column 8, lines 3-11; figure 3C, segment 118; object program segments to control the manner in which an associated file is presented and manipulated to a particular user),

configured to:

associate the control access data structure with the object (see column 8, lines 25-44; figure 3C, segment 120; a data segment containing the digital signature of the program authorization information); and associate the authorized security principal with the object and with the control access data structure (see column 7, lines 66-68; column 8, lines 1-2; figure 3C, segment 116; specification for the authorization for the object's programs that operate on the object).

As per claim 118, Fischer also explains:

the extensible control access right further comprising an access control entry that is associated with the object (see column 8, lines 3-11; figure 3C, segment 118; object program segments to control the manner in which an associated file is presented and manipulated to a particular user),

configured to maintain:

a unique identifier of the control access data structure to associate the control access data structure with the object (see column 8, lines 25-44; figure 3C, segment 120; a data segment containing the digital signature of the program authorization information); and

a unique identifier of the authorized security principal to associate the authorized security principal with the object and with the control access data structure (see column 8, lines 35-44; figure 3C, segment 118; a signature of the program, used to operate on an object, together with the program authorization information (PAI)).

As per claim 119, Fischer illustrates a computing system comprising:

an operating system to manage one or more objects within the computing system (see column 2, lines 16-23; an operating system design which limits the ability of program about to be executed to the use of predefined resources), where an individual object having an access control list of predefined operating system permissions to perform corresponding operations on the individual object (see column 7, lines 49-53; figure 3C; a data structure for a secure exchangeable object; see column 8, lines 3-7; figure 3C, segment 118; with an object programs segment controlling the manner in which the object is operated upon);

an access control entry to identify a security principal, associated with the individual objects as a component of the access control list (see column 8, lines 11-20; figure 3C, segment 118; object programs represented as segments to call programs to operate on the object, such as displaying a purchase order file to a particular recipient); and

an extensible access right to define access to one or more operations of the individual object, associated with the access control entry such that the security principal is authorized to access the one or more operations of the individual object (see column 8, lines 11-20; figure 3C, segment 118; logical statements to accommodate different uses of the object as extensible access rights associated with; see column 7, lines 66-68; column 8, lines 1-2; figure 3C, segment 116; a specification for the authorization of the object's programs to perform operations on the object).

As per claim 120, Fischer further elaborates on an application to generate a control access data structure that defines the extensible access right (see column 11, lines 7-9; figures 6-9; a utility program for establishing program authorization information).

As per claim 121, Fischer then shows:

a control access data structure that defines the extensible access right (see column 5, lines 3-7; figure 2; a program authorization information (PAI) data structure; column 5, lines 55-67; figure 2, segments 34 and 36; with segments to identify functions on specific files and/or class of files),

configured to maintain a unique identifier of the individual object (see column 5, lines 63-66; figure 2, segment 36; specific user files designated in a segment).

As per claim 122, Fischer additionally mentions:

a control access data structure that defines the extensible access right (see column 5, lines 3-7; figure 2; a program authorization information (PAI) data structure; column 5, lines 55-67; figure 2, segments 34 and 36; with segments to identify functions on specific files and/or class of files),

configured to maintain a unique identifier of the individual object (see column 5, lines 63-66; figure 2, segment 36; specific user files designated in a segment), and

wherein the access control entry is configured to maintain a unique identifier of the control access data structure to associate the control access data structure with the individual object and with the security principal (see column 8, lines 35-44; figure 3C, segment 118; a signature of the program, used to operate on an object, together with the program authorization information (PAI)).

As per claim 123, Fischer also suggests:

that the access control entry is configured to maintain a unique identifier of the security principal to associate the security principal with the individual object (see column 7, lines 66-68; column 8, lines 1-2; figure 3C, segment 116; specification for the authorization for the object's programs that operate on the object).

As per claim 124, Fischer then describes:

that the extensible access right further defines access to a property of the individual object (see column 8, lines 13-16; access to a particular version of a digital purchase order as a property of an object accessible depending upon the user).

As per claim 125, Fischer moreover shows:

that the extensible access right further defines access to a method exposed by the individual object (see column 5, lines 55-61; figure 2, segments 34; a segment that specifies the kind of access and use of a file like a program and the particular files; see column 6, lines 8-10; such as alter a program file).

As per claim 126, Fischer next points out:

that the extensible access right further defines access to a property of the individual object (see column 8, lines 13-16; access to a particular version of a digital purchase order as a property of an object accessible depending upon the user),

associated with the access control entry such that the security principal is authorized to access the property of the individual object (see column 7, lines 66-68; column 8, lines 1-2;

figure 3C, segment 116; specification for the authorization for the object's programs that operate on the object to access the object's property).

As per claim 127, Fischer also discusses:

that the extensible access right further defines access to a method exposed by the individual object (see column 5, lines 55-61; figure 2, segments 34; a segment that specifies the kind of access and use of a file like a program and the particular files; see column 6, lines 8-10; such as alter a program file),

associated with the access control entry such that the security principal is authorized to initiate the method (see column 7, lines 66-68; column 8, lines 1-2; figure 3C, segment 116; specification for the authorization for the object's programs that operate on the object).

As per claim 128, Fischer further points out:

a control access data structure that defines the extensible access right (see column 5, lines 55-58; figure 2, segment 34; a program authorization information (PAI) data structure identifying types of functions and resources), and

wherein the extensible access right can be redefined with a change of values maintained by the control access data structure (see column 11, lines 40-61; figure 6, steps 212, 214, and 216; determining file access authority with respect to any fields or elements in a file to a particular type of access to the file; see column 11, lines 7-13; by any of the end user, the end user's agent, or even the manufacturer defining a range of authorities in the program authorization information).

As per claim 129, Fischer then shows:

a control access data structure that defines the extensible access right (see column 5, lines 55-58; figure 2, segment 34; a program authorization information (PAI) data structure identifying types of functions and resources), and

wherein the extensible access right can be redefined without a change to the access control entry (see column 6, lines 13-18; figure 2, segment 38; level of authority granted to a set of rights where the right can be changed to another right in the same level of authority).

Conclusion

22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Boebert et al., U.S. Patent No. 4,713,753 A discloses a means and methods for limiting access rights of users to protected system files.
- Stefik, U.S. Patent No. 5,715,403 A describes a system for controlling use and distribution of digital works

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (571) 272-3801, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed **"OFFICIAL FAX"**. Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only **"OFFICIAL FAX"** but also **"AMENDMENT AFTER FINAL"**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100.

June 10, 2005

Justin Darrow
JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100

approved.
Bruell, Act'g DIRECTOR TC2100